Chief Information Officer's Section
Office of the Governor
State of Utah

September 16 2002

State Firewall Policy

Policy Objectives and Scope: This policy is to state the need, define common terms, and define standards for implementing and maintaining network firewalls by State agencies.

Definitions:

Firewall: Security systems that control and restrict network connectivity and network services.

Service: An application or listener enabled to accept client connections. Examples of services include file transfer protocol (FTP) and Web browsing (HTTP).

Agency Security Manager: A role filled by one or more individuals to ensure that agencies comply with required policies and procedures, follow industry best practices, and manage agency security requirements.

Need for Firewalls:

Due to the open nature of network connectivity, measures must be implemented to prevent unauthorized access to network services and deny disclosure of internal network information.

Implementation:

Approval Process: Permission to enable paths will be granted by the agency security manager only when the paths are necessary for business reasons and adequate security measures will be used.

Default To Denial: State of Utah firewalls must block every network connectivity path and network service not specifically authorized by the agency security manager.

Firewall Physical Security: State agencies must employ due diligence in ensuring physical security at any location where firewalls will be installed.

Change Control:

Approval Process: Configuration changes and software modifications must follow agency or State production change control procedures.

Firewall Access Privileges: Privileges to modify the functionality, connectivity, and services supported by firewalls must be restricted to individuals authorized by the agency security manager. At the agency's request, the ITS NOC (Network Operations Center) may be retained to make changes.

Change Control Logging: All changes to firewall configuration parameters, enabled services, and permitted connectivity must be logged.

Ongoing Operational Concerns:

Logs: System activity must be logged. Logs should be available for review and retained in accordance with agency retention policies.

Periodic Review: Firewall configuration must be reviewed to ensure compliance to agency or State security policy. Supporting documentation must exist for all enabled services. Agencies are responsible for testing their firewall configuration(s) for effectiveness.

Posting Updates: State of Utah firewalls will run the most current, stable version of software. Agency personnel responsible for managing firewalls will subscribe to security advisories and other relevant sources providing up-to-date information about firewall vulnerabilities.

References:

Interim Date: July 26, 2002
Organization Sponsoring the Standard: ITS, State Information Security Committee (SISC)
State Technical Architect Approval Date: Pending
CIO Approval Date: Pending
ITPSC Presentation Date: 6/27/02 for comment, 8/1/02 for approval, 9/16/02 revised
Author(s): Robert Woolley, John Malouf, Rick Gee (ITS), SISC (State Information Security Committee)
Related Documents: State Information Security Policy, State Network Access Policy RFC 2979 Internet Firewalls